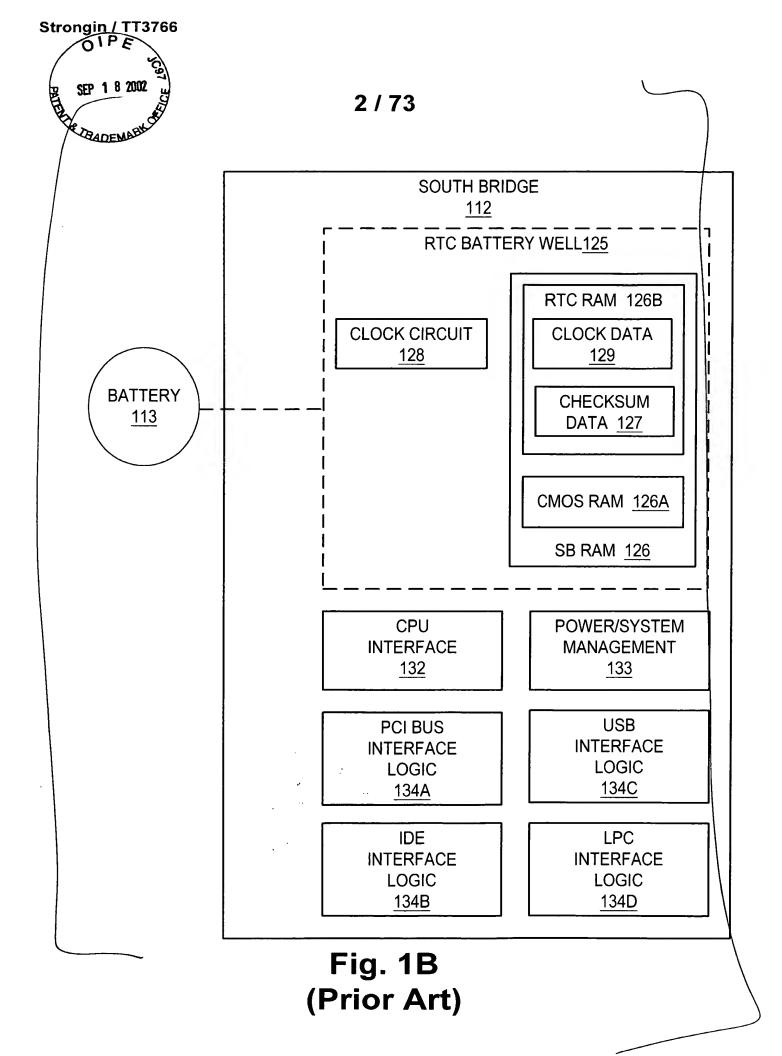


Fig. 1A (Prior Art)



SEP 1 8 2002

RADEMAR

POWER SUPPLY INITIALIZATION POWER SUPPLY GENERATES A POWER GOOD SIGNAL TO THE NORTH BRIDGE 136

UP RECEIVING THE POWER GOOD SIGNAL, THE SOUTH BRIDGE STOPS ASSERTING THE RESET SIGNAL FOR THE PROCESSOR 138

THE PROCESSOR READS THE DEFAULT JUMP LOCATION, USUALLY AT FFFF0h 140

THE PROCESSOR JUMPS TO THE BIOS CODE LOCATION IN THE ROM BIOS, COPIES THE BIOS CODE TO RAM, AND BEGINS PROCESSING BIOS CODE INSTRUCTIONS FROM RAM 142

BIOS CODE PERFORMS POWER ON SELF TEST (POST) 144

BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 146

BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 148

BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 150

BIOS CODE IDENTIFIES THE BOOT LOCATION 152

BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 154

Fig. 2A (Prior Art)

INTERRUPT CONTROLLER RECEIVES A REQUEST FOR SYSTEM MANAGEMENT MODE (SMM) 172

INTERRUPT CONTROLLER SIGNALS THE REQUEST FOR SMM TO THE PROCESSOR BY ASSERTING THE SYSTEM MANAGEMENT INTERRUPT (SMI#) SIGNAL 174

PROCESSOR RECOGNIZES THE REQUEST FOR SMM AND ASSERTS THE SMI ACTIVE (SMIACT#) SIGNAL 176

SYSTEM RECOGINIZES THE SMIACT# SIGNAL, DISABLES ACCESS TO RAM, AND ENABLES ACCESS TO SYSTEM MANAGEMENT RAM (SMRAM) SPACE 178

CURRENT PROCESSOR STATE IS SAVED TO SMRAM 180

PROCESSOR RESETS TO SMM DEFAULT STATE AND ENTERS SMM 182

PROCESSOR READS DEFAULT POINTER AND JUMPS INTO SMRAM SPACE 184

STATUS REGISTERS ARE CHECKED TO IDENTIFY THE SMI REQUEST 186

SMI HANDLER SERVICES THE SMI REQUEST 188

SMI HANDLER ISSUES RETURN FROM SMM (RSM) INSTRUCTION TO PROCESSOR 190

PROCESSOR RESTORES SAVED STATE INFORMATION AND CONTINUES
NORMAL OPERATION 192

Fig. 2B (Prior Art)

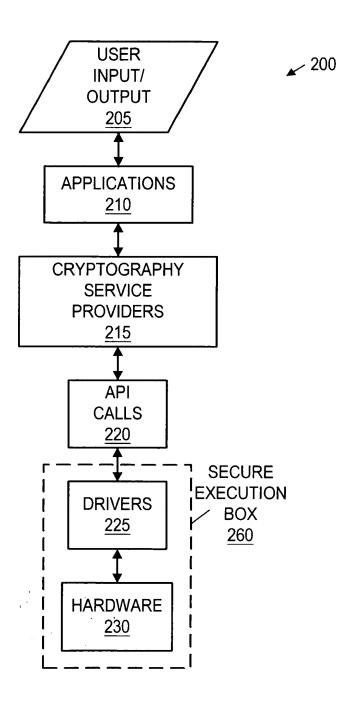
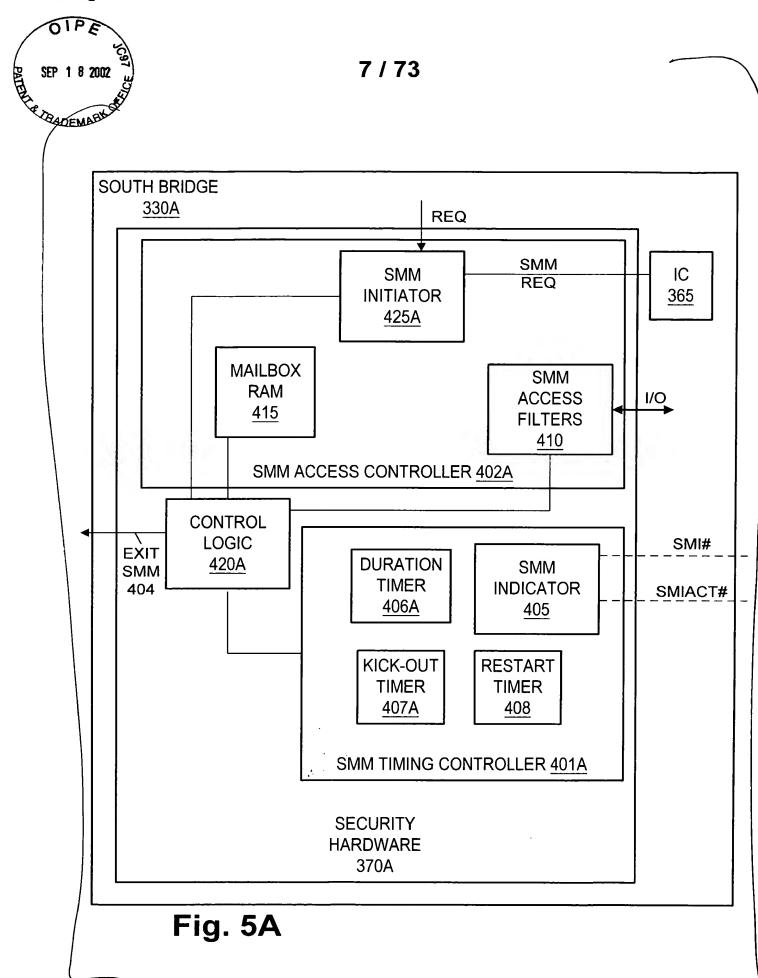
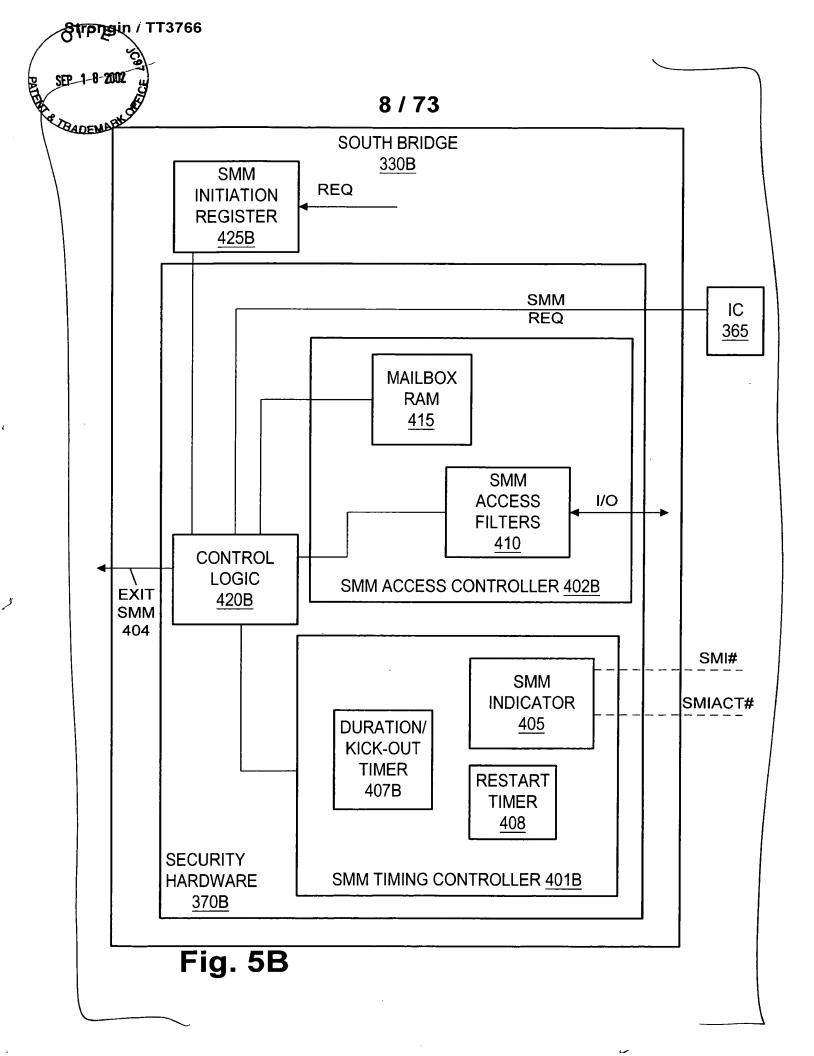


Fig. 3 2





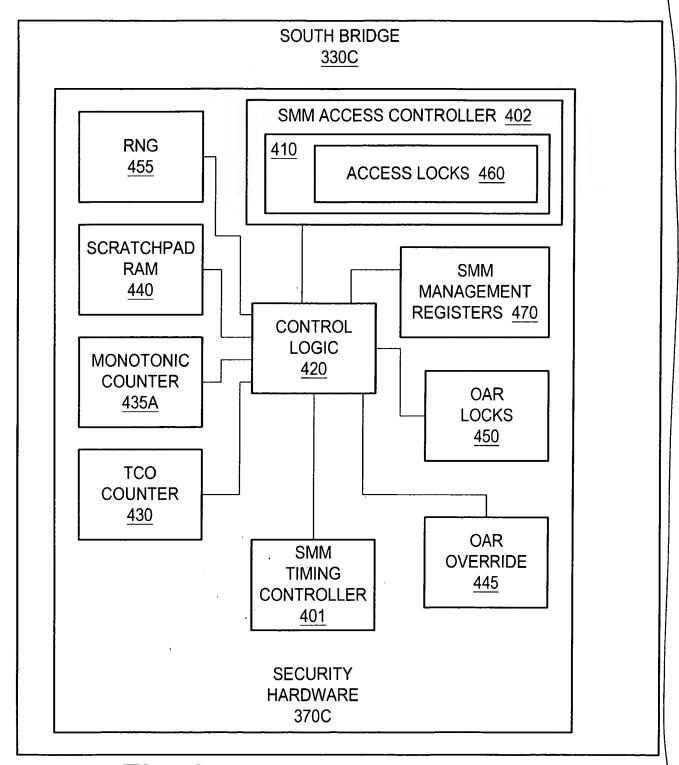
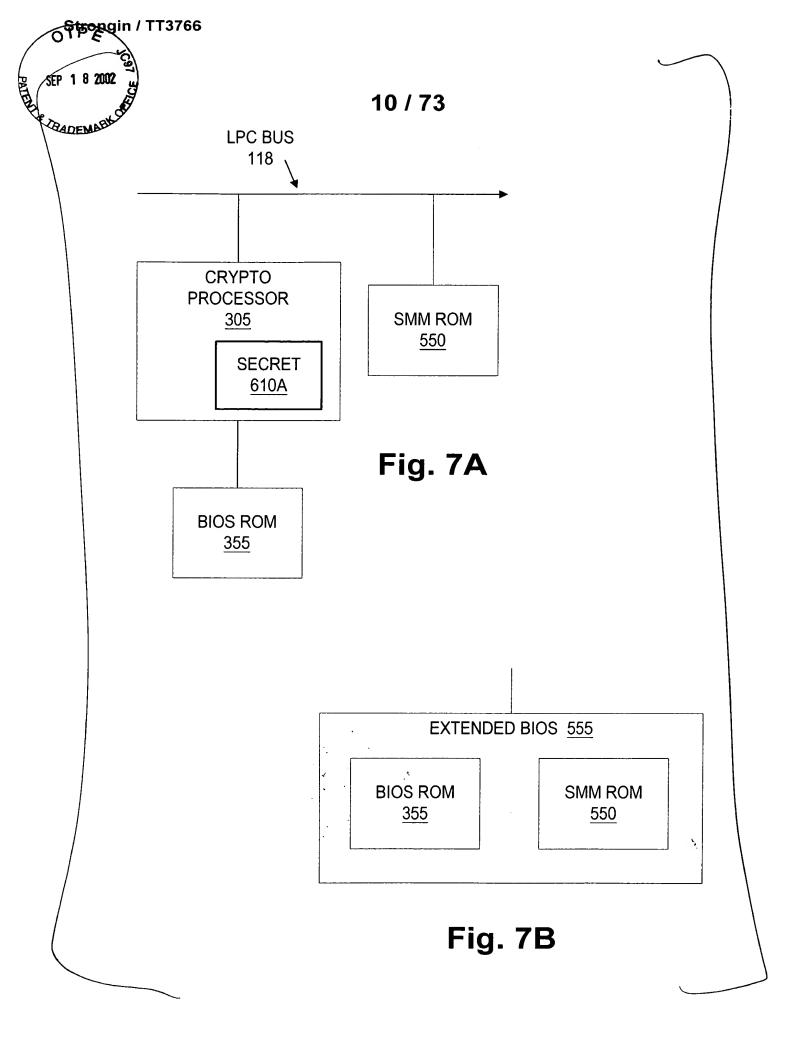


Fig. 6



11 / 73

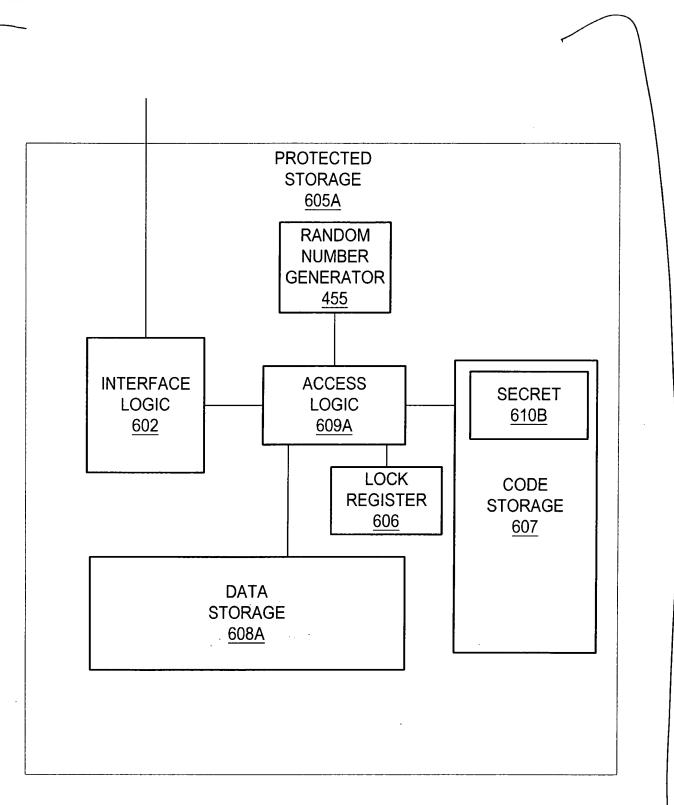
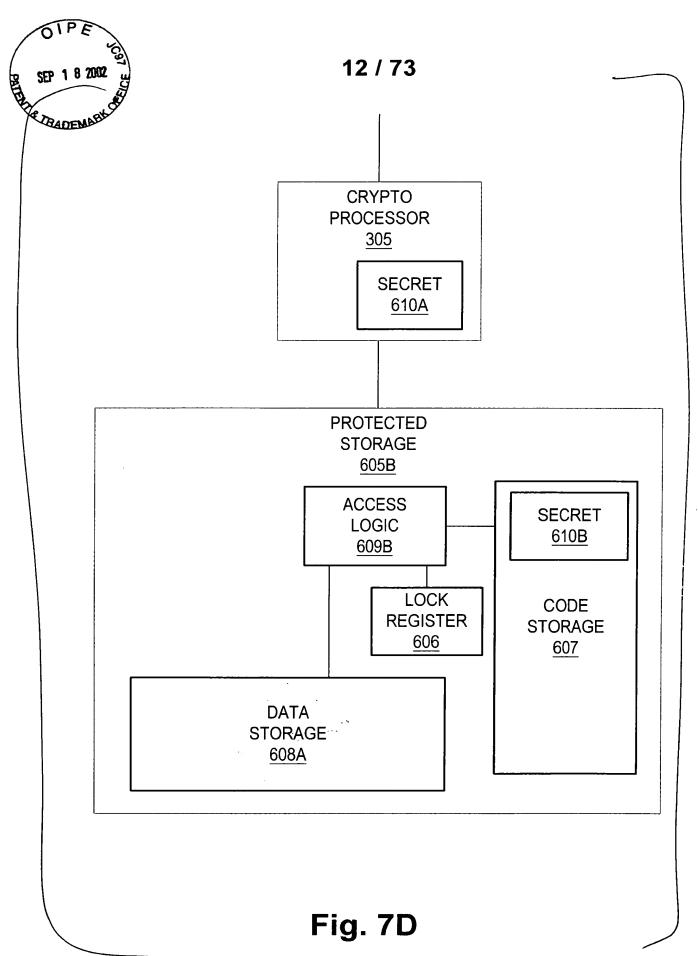
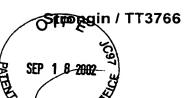


Fig. 7C





SMM ROM <u>550</u> PUBLIC 0 SECRET 610D <u>625</u> SMM ROM 0 PUBLIC 1 615 630 SMM ROM 1 **RESERVED** <u>616</u> <u>635</u> SMM ROM 2 **REGISTERS** <u>617</u> 640 MONOTONIC COUNTER 435B

Fig. 8B

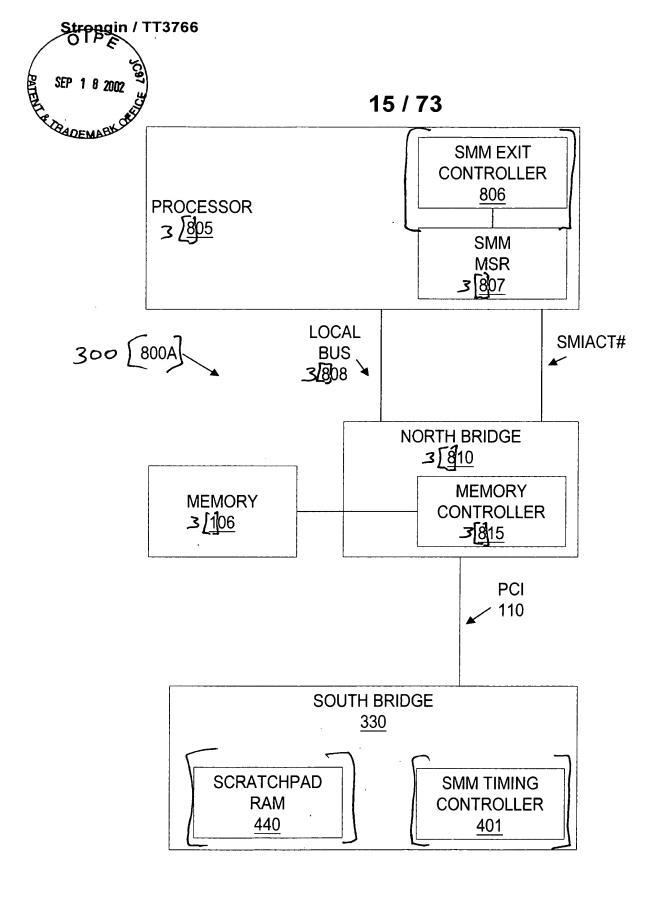
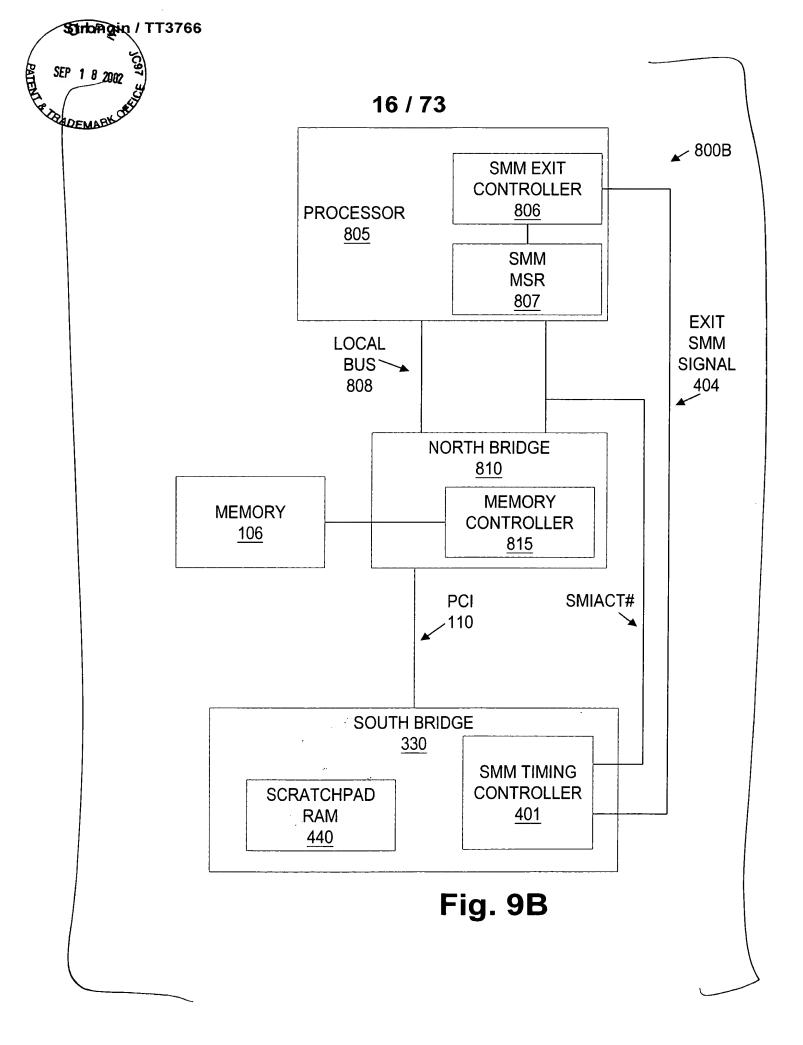
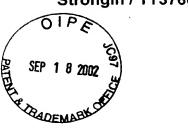


Fig. 9A 3







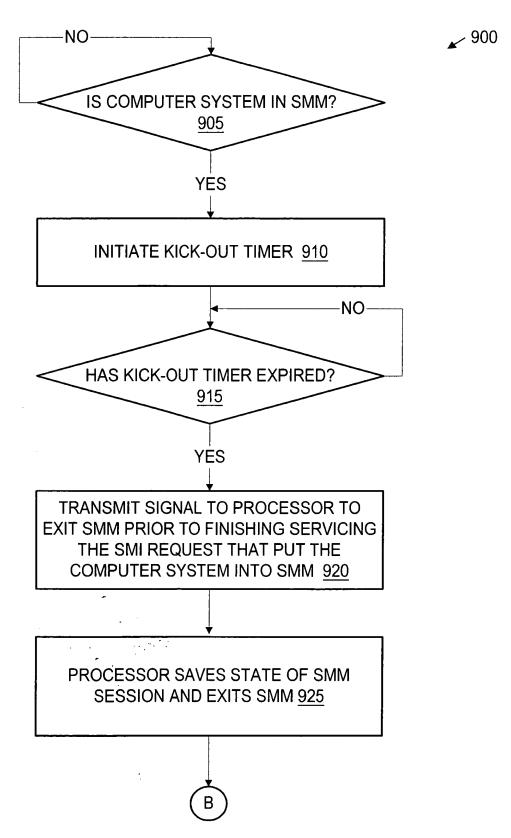
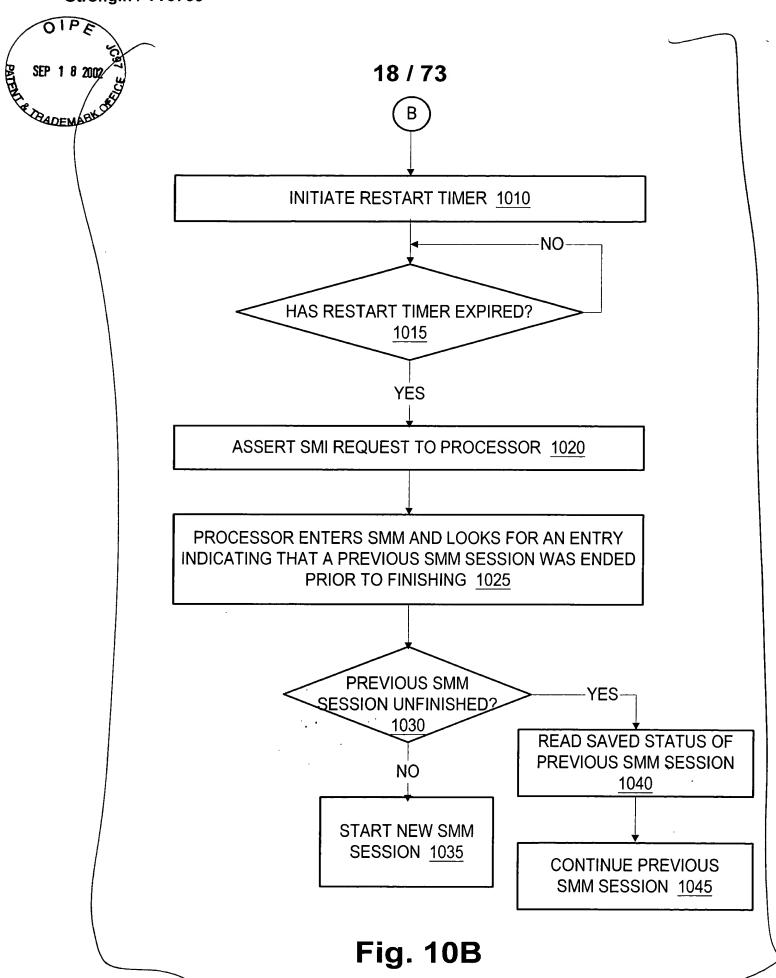
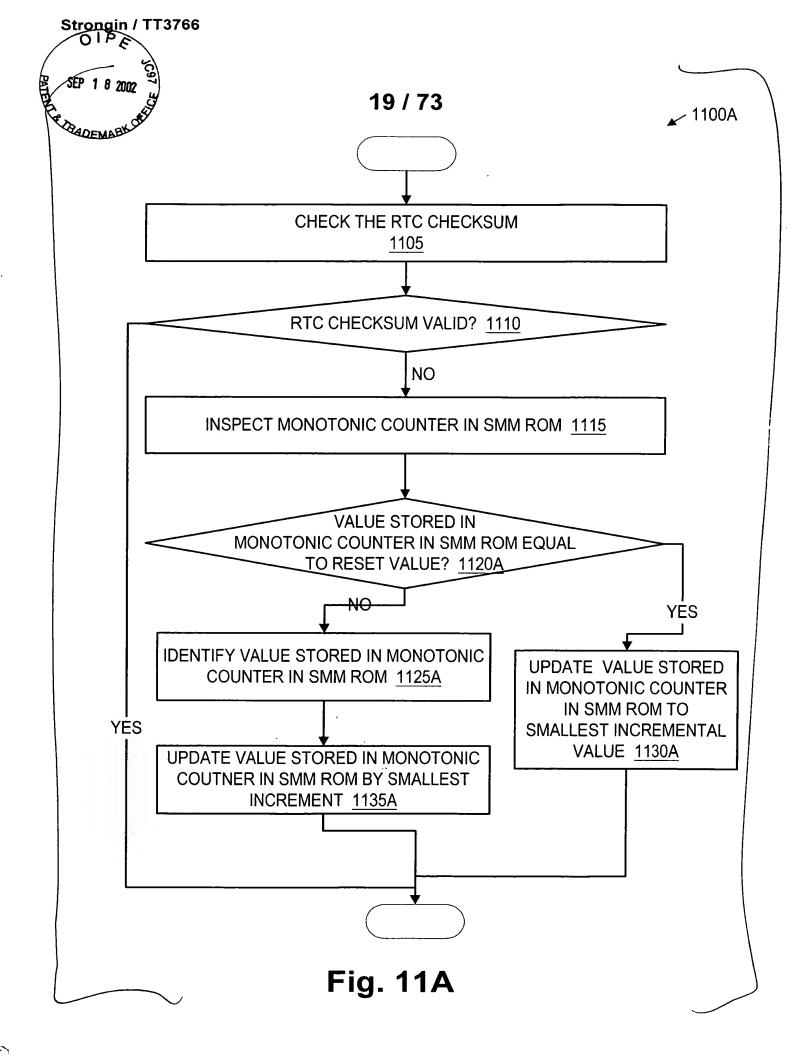
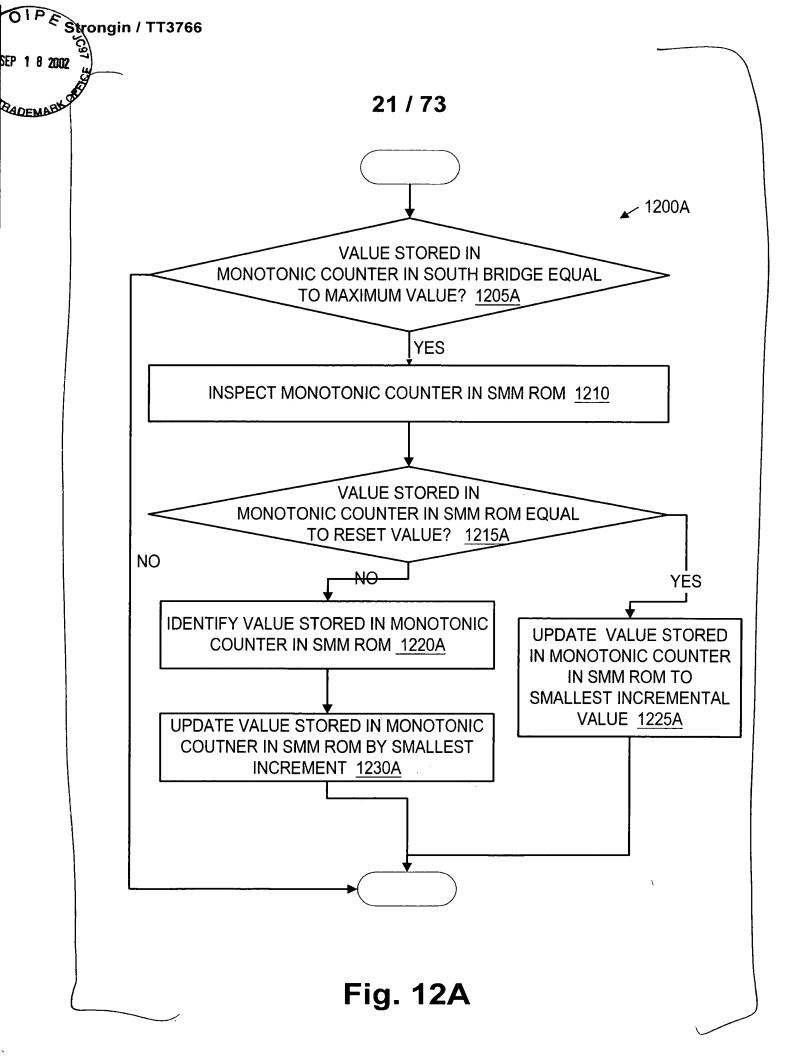
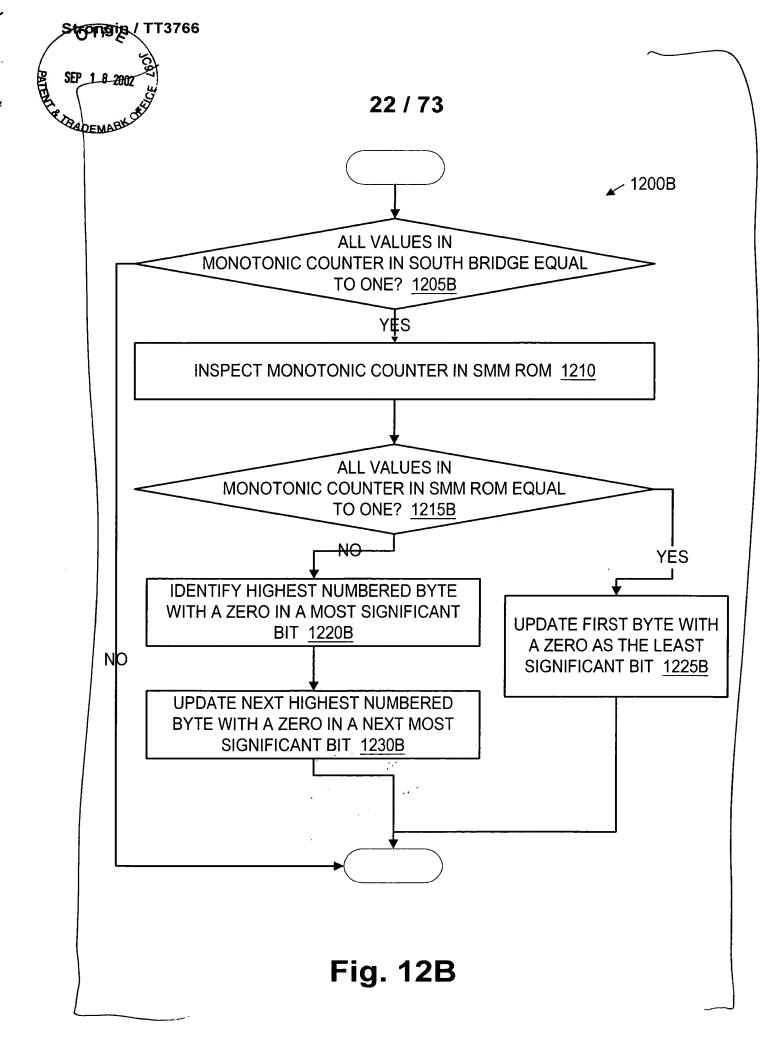


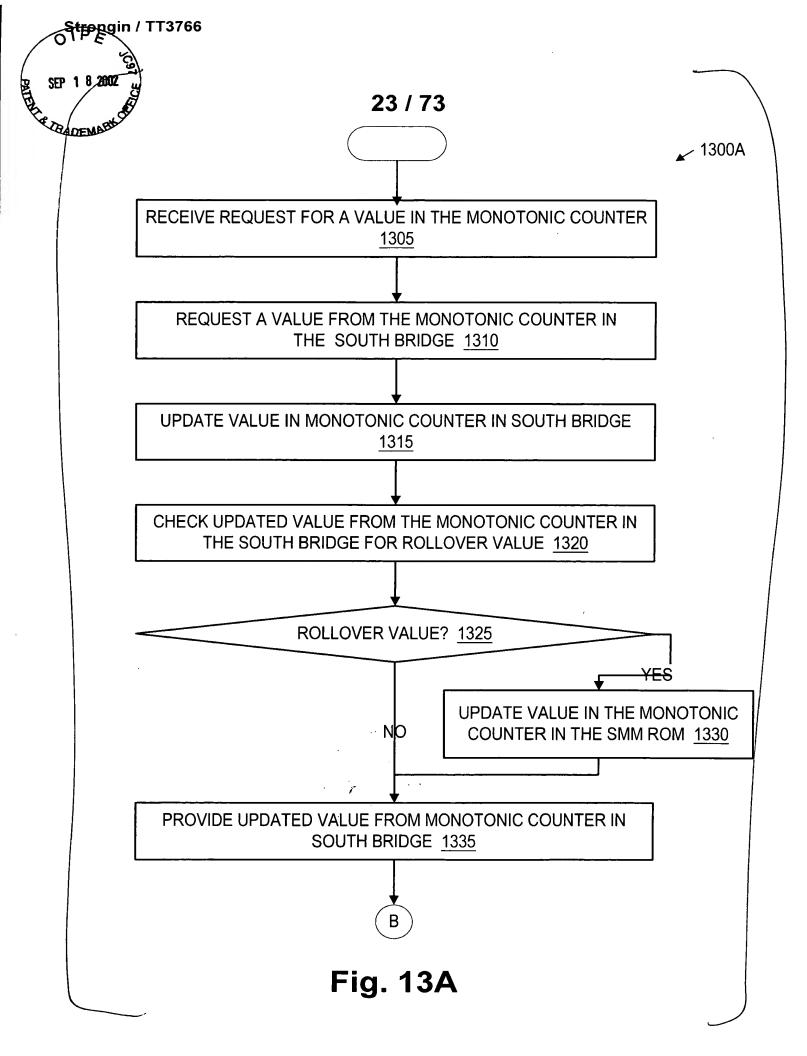
Fig. 10A











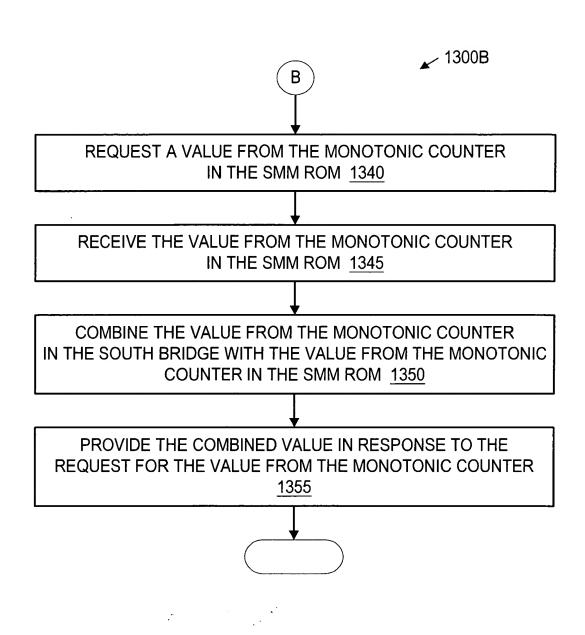


Fig. 13B

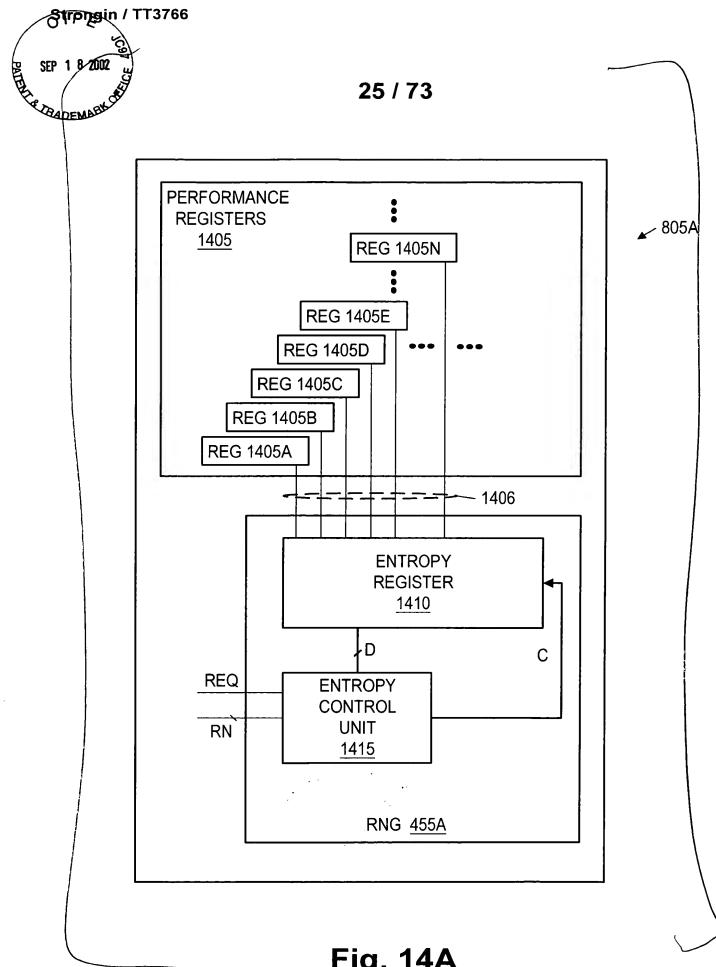
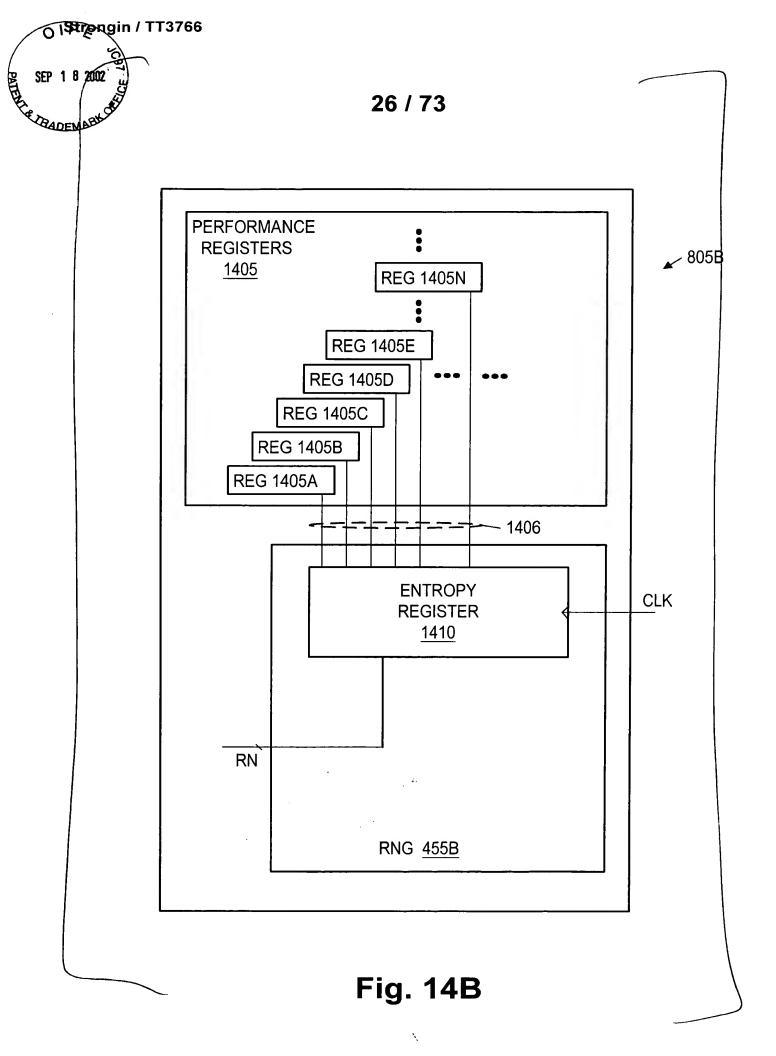
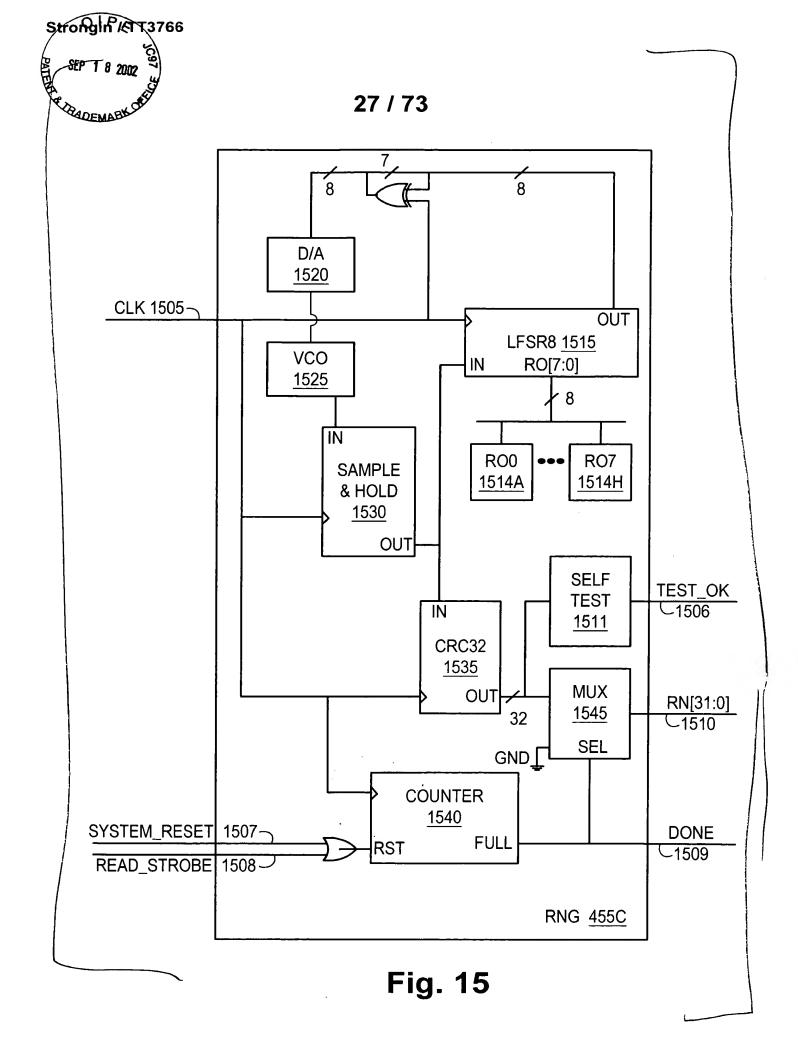


Fig. 14A



i



RADEMARY

___ 1600A

THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620

BIOS CODE PERFORMS POWER ON SELF TEST (POST) 1625

ACCESSING THE SECURITY HARDWARE 1630

OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632

BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635

BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 1640

BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645

CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

BIOS CODE IDENTIFIES THE BOOT LOCATION 1655

BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16A



1600B

OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615

THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM $\ \underline{1620}$

ACCESSING THE SECURITY HARDWARE 1630

OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632

BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635

BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645

CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

BIOS CODE IDENTIFIES THE BOOT LOCATION 1655

BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16B

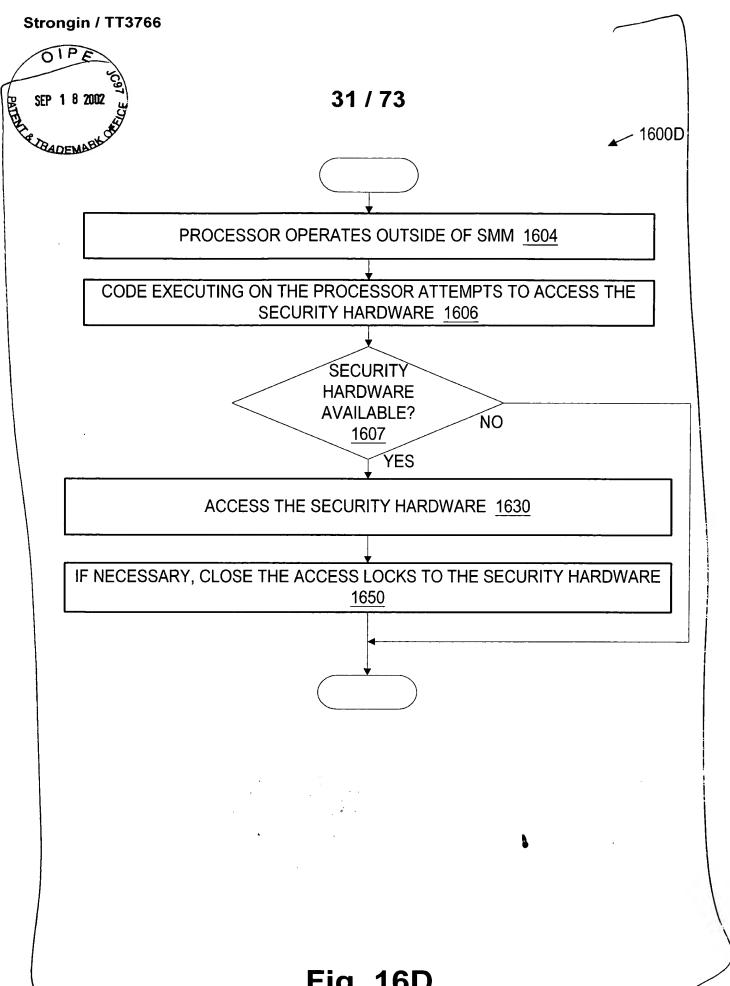
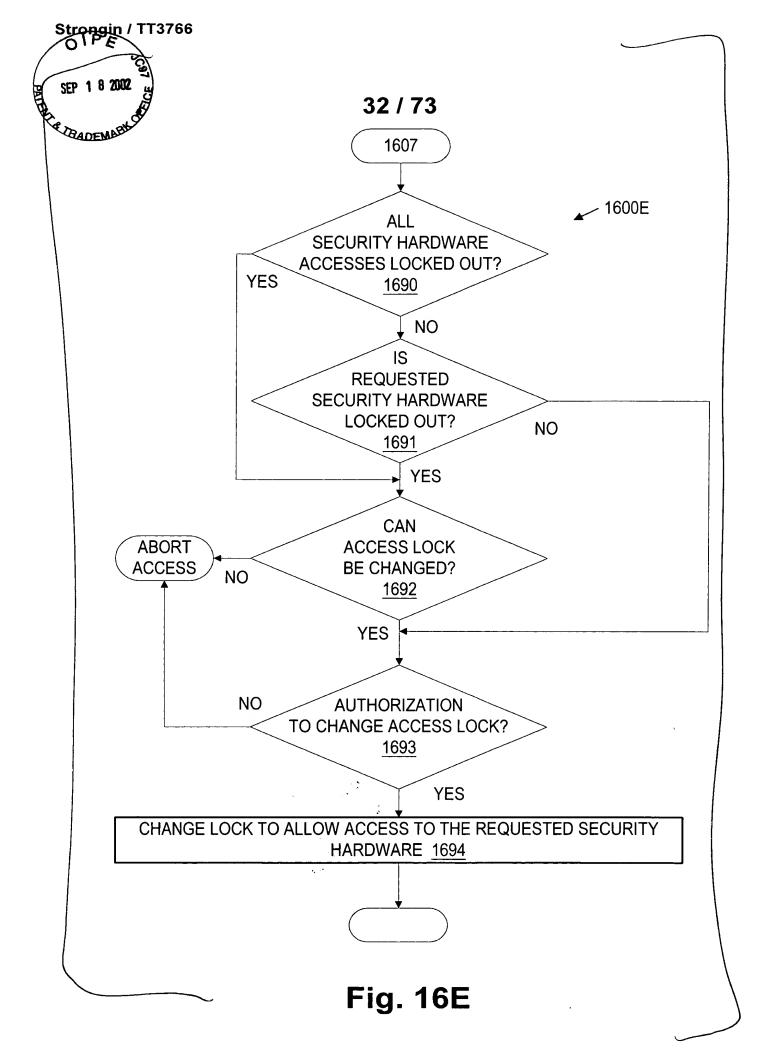


Fig. 16D



SEP 1 8 2002

___ 1600F

THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE **RAM 1605**

OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615

THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620

ACCESSING THE SECURITY HARDWARE 1630

CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

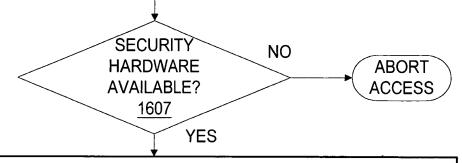
THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES **OPERATING 1665**

Fig. 16F



✓ 1600G

THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM 1605



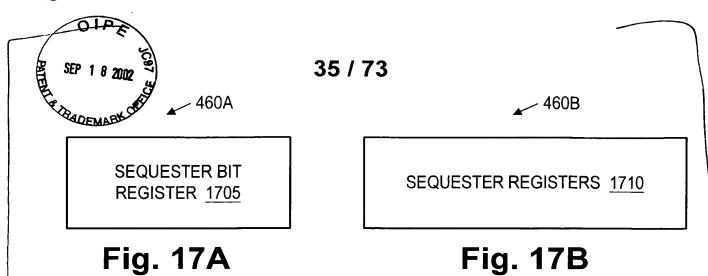
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM $\,\underline{1620}$

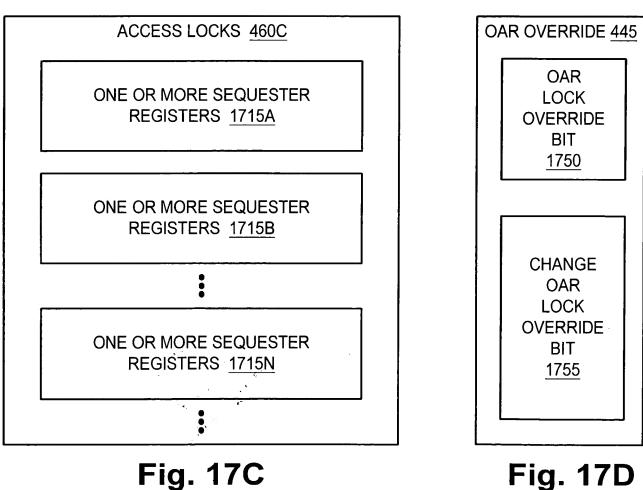
ACCESSING THE SECURITY HARDWARE 1630

CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING 1665

Fig. 16G





BIT 1755 Fig. 17D

OAR

LOCK

OVERRIDE BIT 1750

CHANGE OAR LOCK **OVERRIDE**



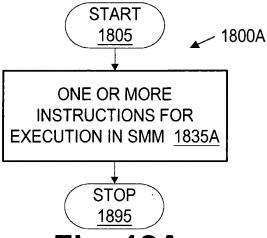


Fig. 18A PRIOR ART

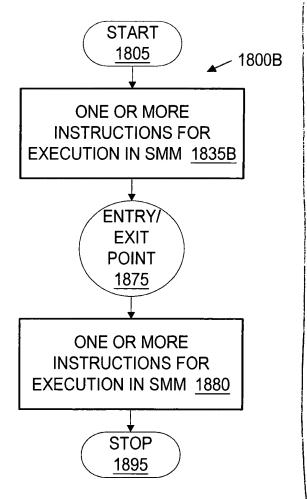
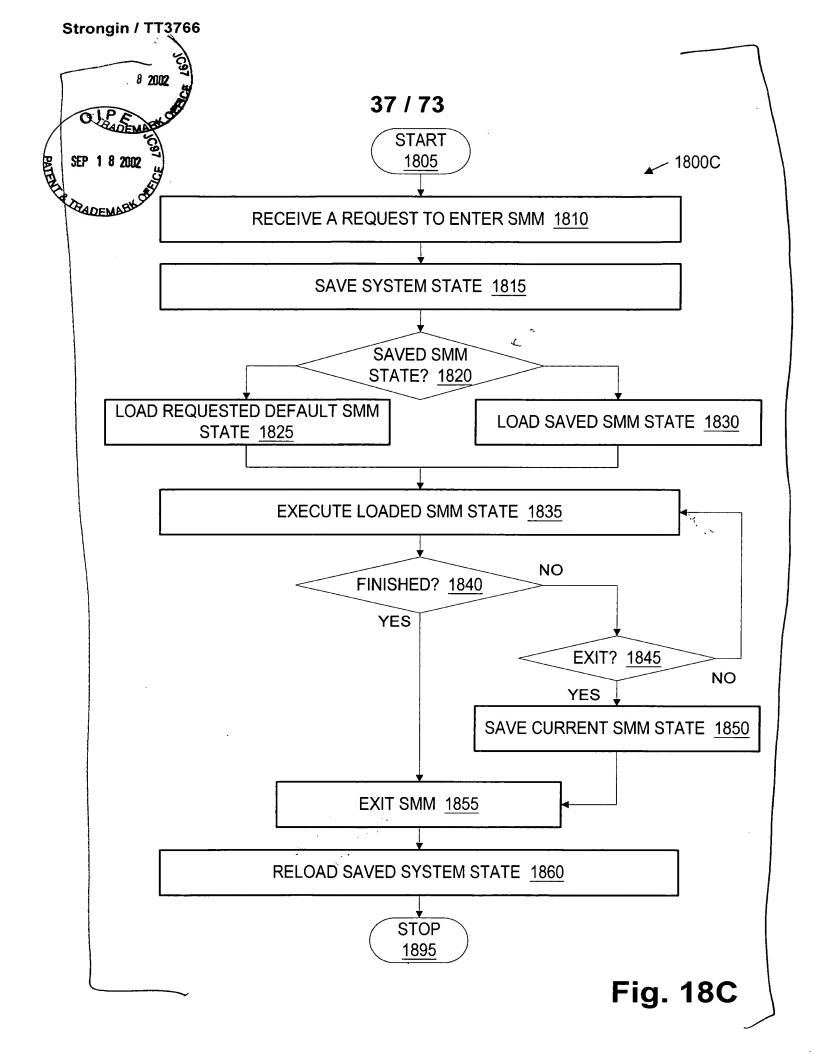
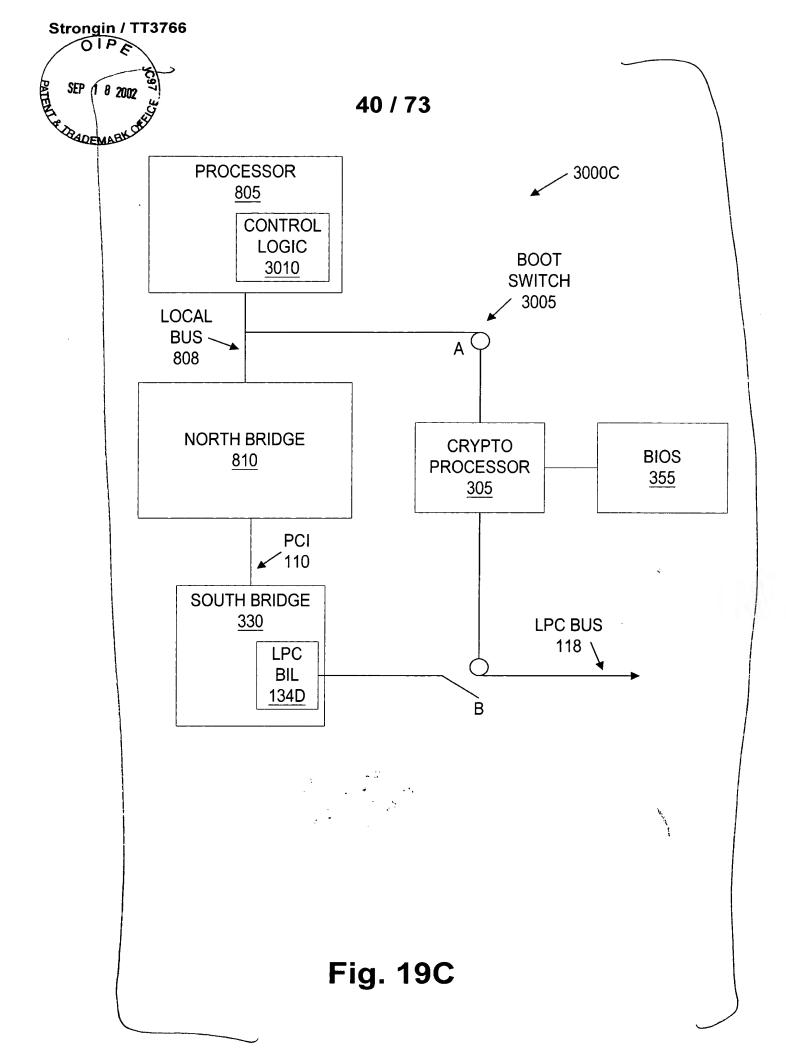
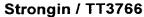


Fig. 18B









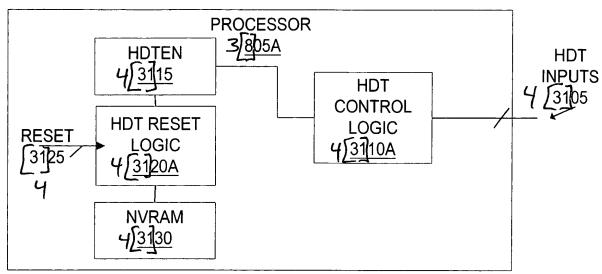
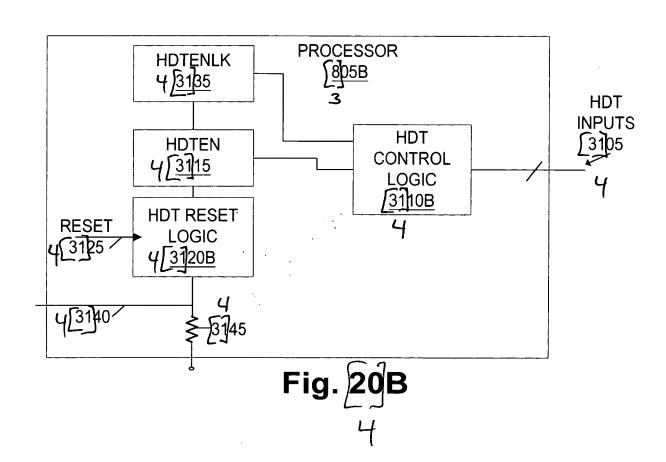
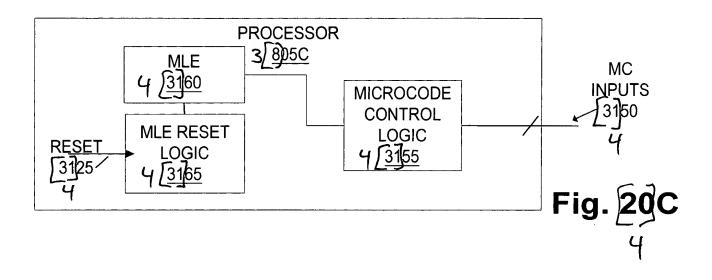
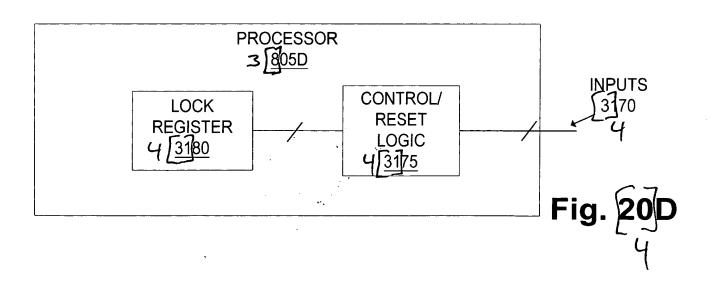


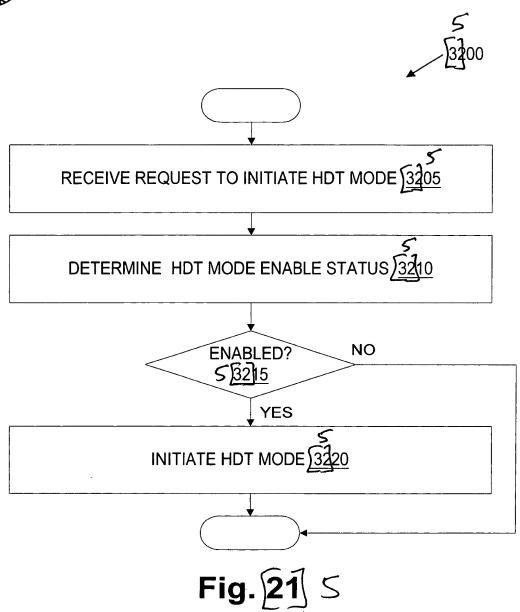
Fig. 20A











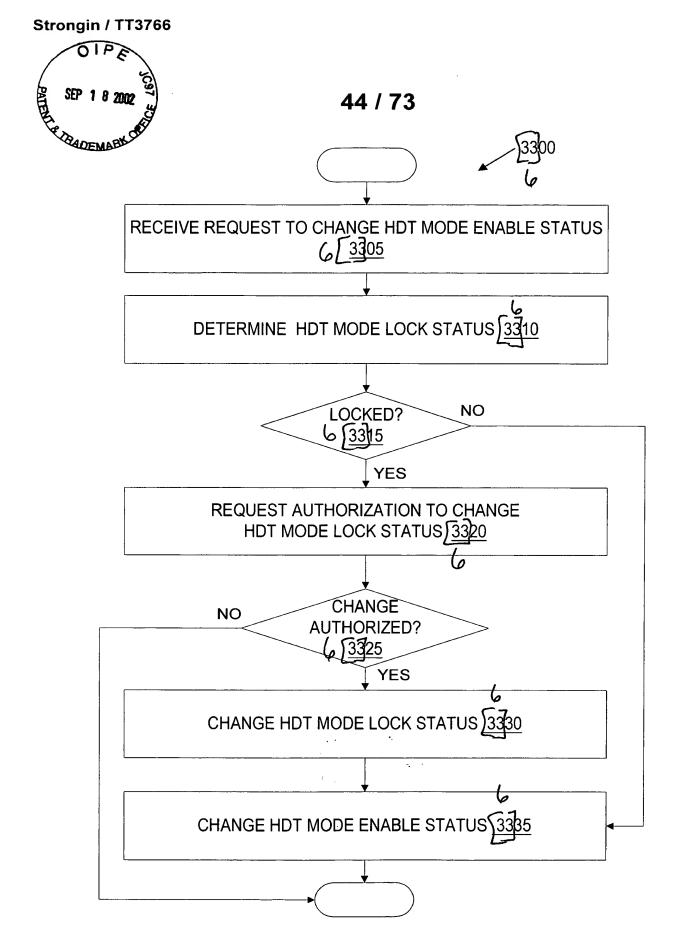
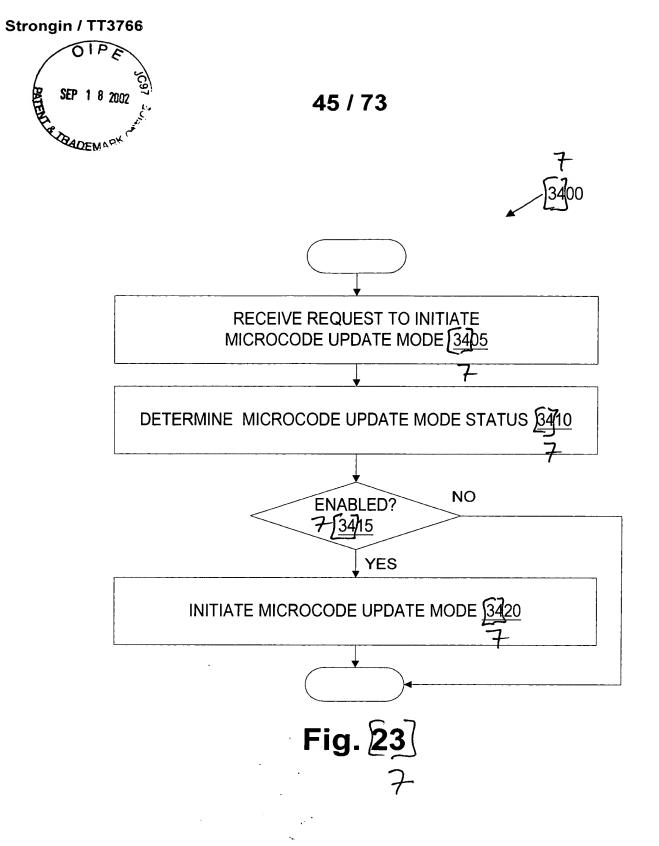


Fig. 22 6



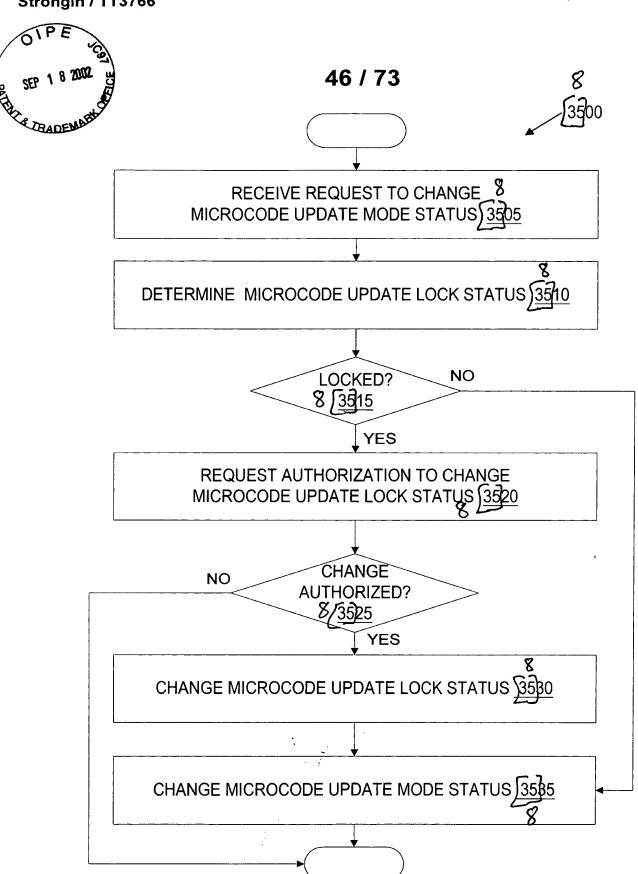


Fig. 24



3600A

A SECURITY DEVICE RECEIVES A TRANSACTION REQUEST FOR A STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3605A

THE SECURITY DEVICE PROVIDES ACCESS CONTROL FOR THE STORAGE DEVICE 3610A

THE SECURITY DEVICE MAPS THE STORAGE LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE STORAGE DEVICE 3615A

THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3620A

THE STORAGE DEVICE PERFORMS THE REQUESTED TRANSACTION 3625A

Fig. 25A

3600B

A CRYPTO-PROCESSOR RECEIVES A TRANSACTION REQUEST FOR A MEMORY LOCATION ASSOCIATED WITH A MEMORY CONNECTED TO THE CRYPTO-PROCESSOR 3605B

THE CRYPTO-PROCESSOR PROVIDES ACCESS CONTROL FOR THE MEMORY 3610B

THE CRYPTO-PROCESSOR MAPS THE MEMORY LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE MEMORY 3615B

THE CRYPTO-PROCESSOR PROVIDES THE TRANSACTION REQUEST TO THE MEMORY 3620B

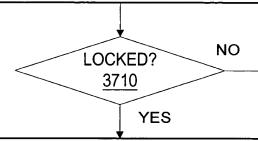
THE MEMORY PERFORMS THE REQUESTED TRANSACTION 3625B

Fig. 25B



- 3610A

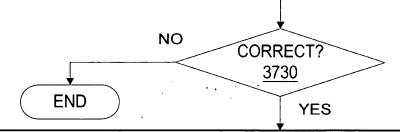
THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION 3705



THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3715

THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE 3720

THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE 3725



THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3735

3620

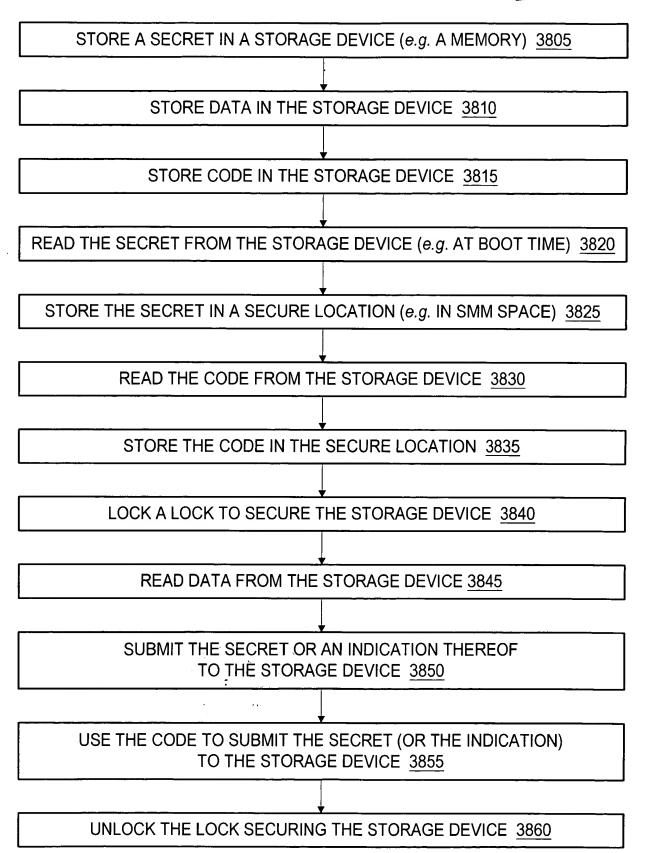


Fig. 27

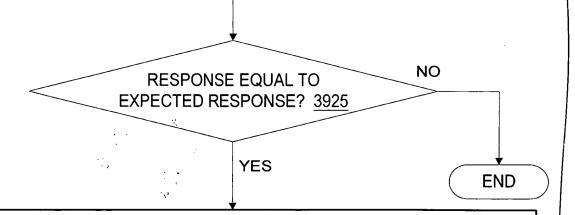
- 3900

A REQUESTOR MAKES AN ACCESS REQUEST 3905

A GATEKEEPER RECEIVES THE ACCESS REQUEST AND PROVIDES A CHALLENGE TO THE REQUESTOR TO AUTHENTICATE THE REQUESTOR'S AUTHORITY TO MAKE THE ACCESS REQUEST 3910

THE REQUESTOR RECEIVES THE CHALLENGE AND PROVIDES A RESPONSE TO THE CHALLENGE TO AUTHENTICATE THE REQUESTOR'S AUTHORITY TO MAKE THE ACCESS REQUEST 3915

THE GATEKEEPER RECEIVES THE RESPONSE TO THE CHALLENGE AND COMPARES THE RESPONSE TO AN EXPECTED RESPONSE 3920



THE GATEKEEPER APPROVES THE ACCESS REQUEST 3930

Fig. 28 (Prior Art)

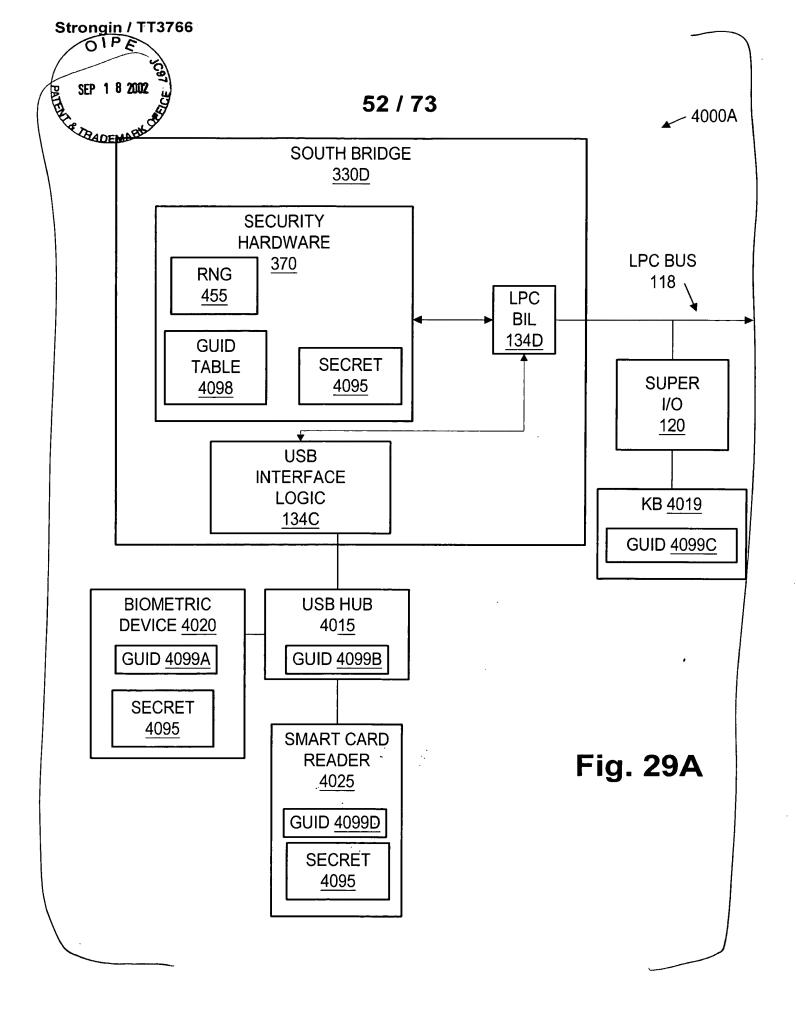
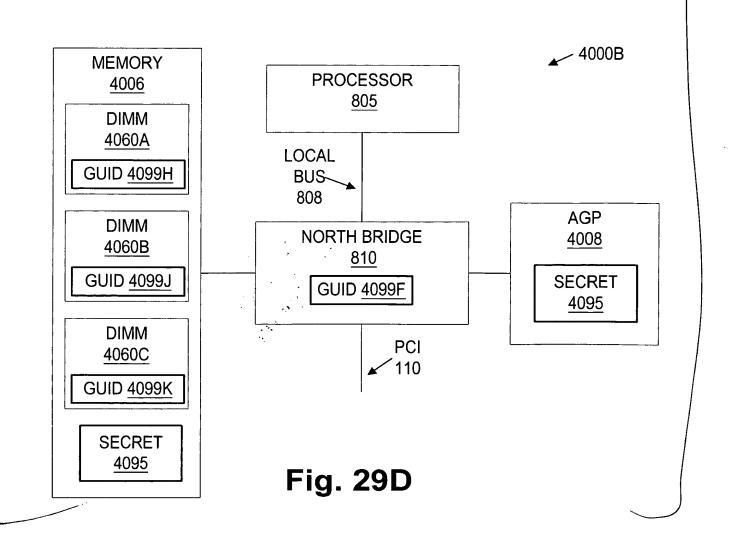


Fig. 29B

Fig. 29C



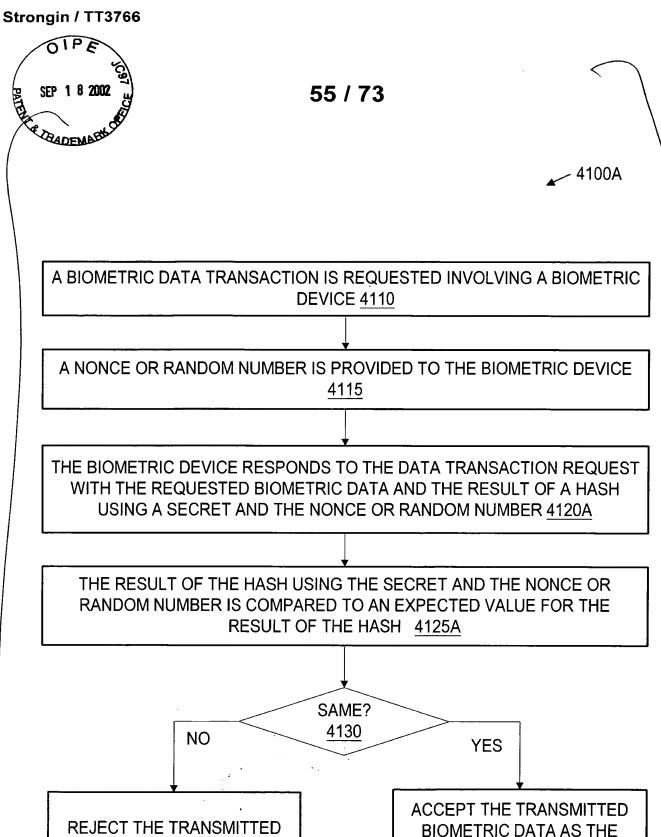


Fig. 30A

BIOMETRIC DATA 4135

REQUESTED BIOMETRIC DATA

4140

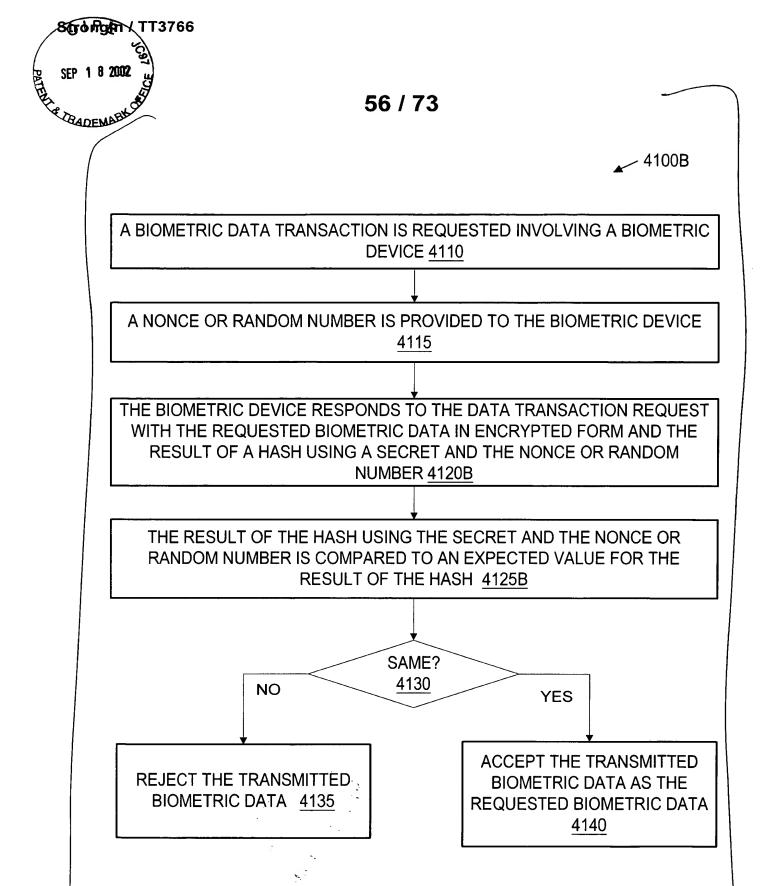


Fig. 30B

Fig. 31A



.__ 4200B

SEP 1 8 2002

A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET

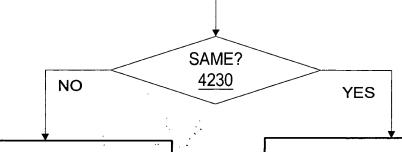
OF VICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP

A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4210

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4215

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY EITHER ENCRYPTING THE REQUESTED DATA USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4220B

THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4225



REJECT THE TRANSMITTED DATA OR DO NOT SENT THE **DATA 4235**

ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND SEND THE ENCRYPTED DATA 4240B

Fig. 31B

PADEMAR'

59 / 73

- 4300A

A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305

A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4320A

THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325

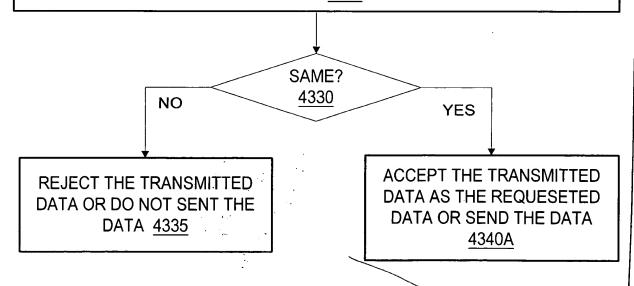
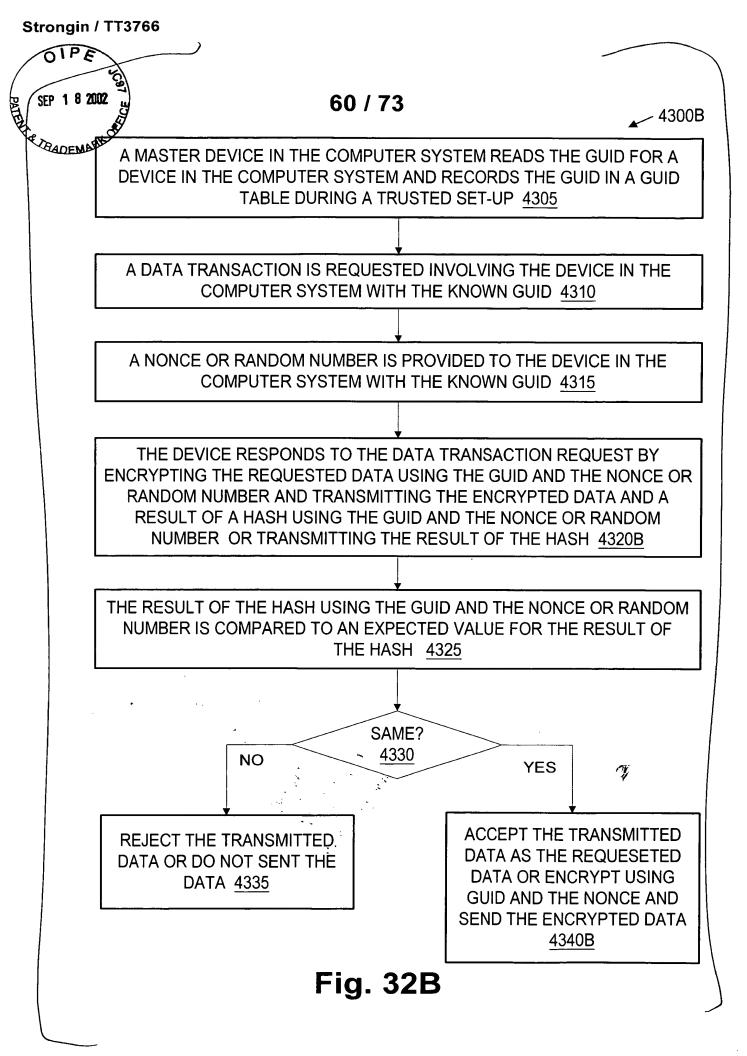


Fig. 32A



SEP 1 8 2002

RADEMA

61 / 73

4300C

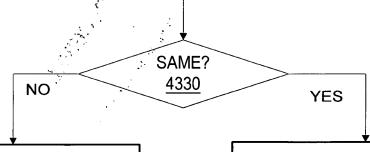
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM, RECORDS THE GUID IN A GUID TABLE, AND TRANSMITS A SECRET TO THE DEVICE DURING A TRUSTED SET-UP 4306

A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET 4311

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET 4316

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320C

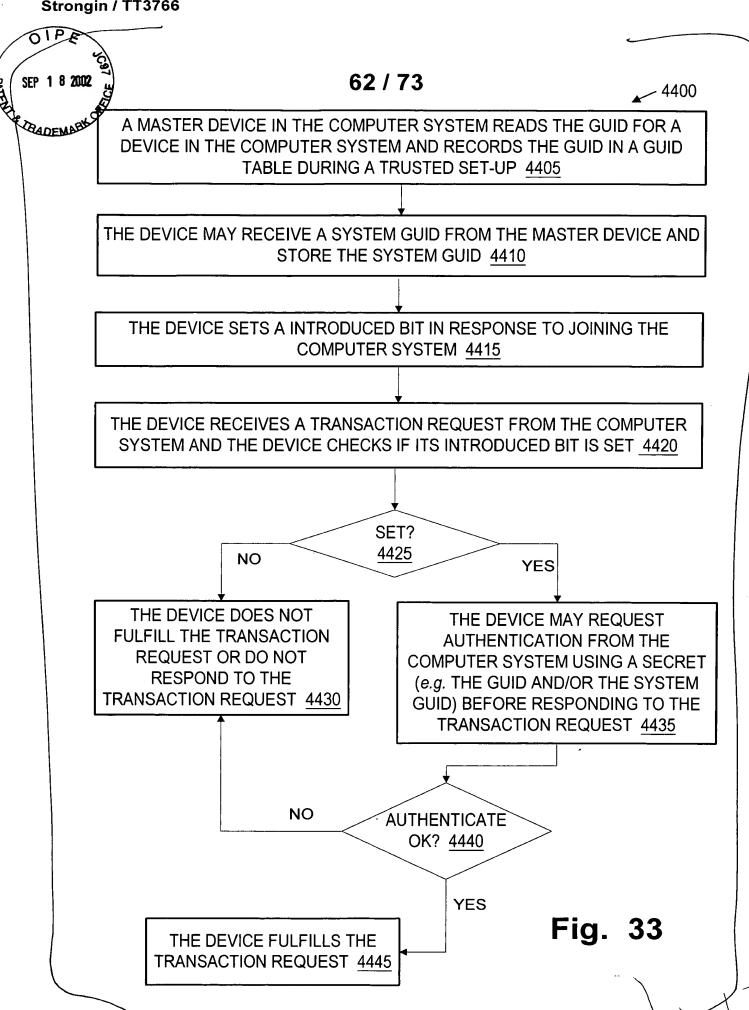
THE RESULT OF THE HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4326



REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335

Fig. 32C

ACCEPT THE TRANSMITTED
DATA AS THE REQUESETED
DATA OR ENCRYPT USING THE
SECRET, THE GUID, AND THE
NONCE AND SEND THE
ENCRYPTED DATA 4340C





4500

THE DEVICE OR THE MASTER DEVICE INITIATES A REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4505

THE DEVICE AND THE MASTER DEVICE AUTHENTICATE EACH OTHER USING THE GUID AND/OR THE SYSTEM GUID IN RESPONSE TO THE REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4510

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE AND THE MASTER DEVICE SUCCESSFULLY AUTHENTICATING EACH OTHER $\underline{4515}$

Fig. 34

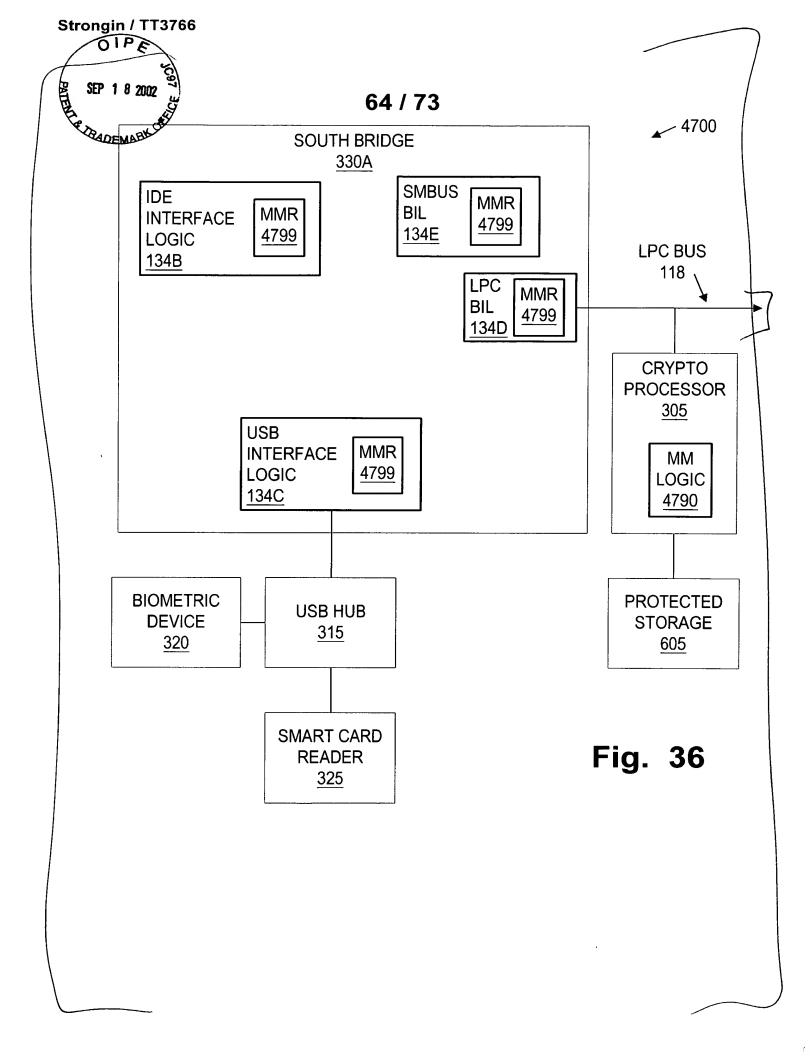
4600

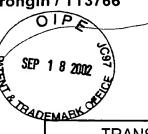
THE DEVICE RECEIVING A COMMAND FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4605

THE DEVICE RECEIVING A MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4610

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE RECEIVING THE MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4615

Fig. 35





~ 4800

TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER 4805

SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM 4810

THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4815

THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS 4820

THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE MASER MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4825

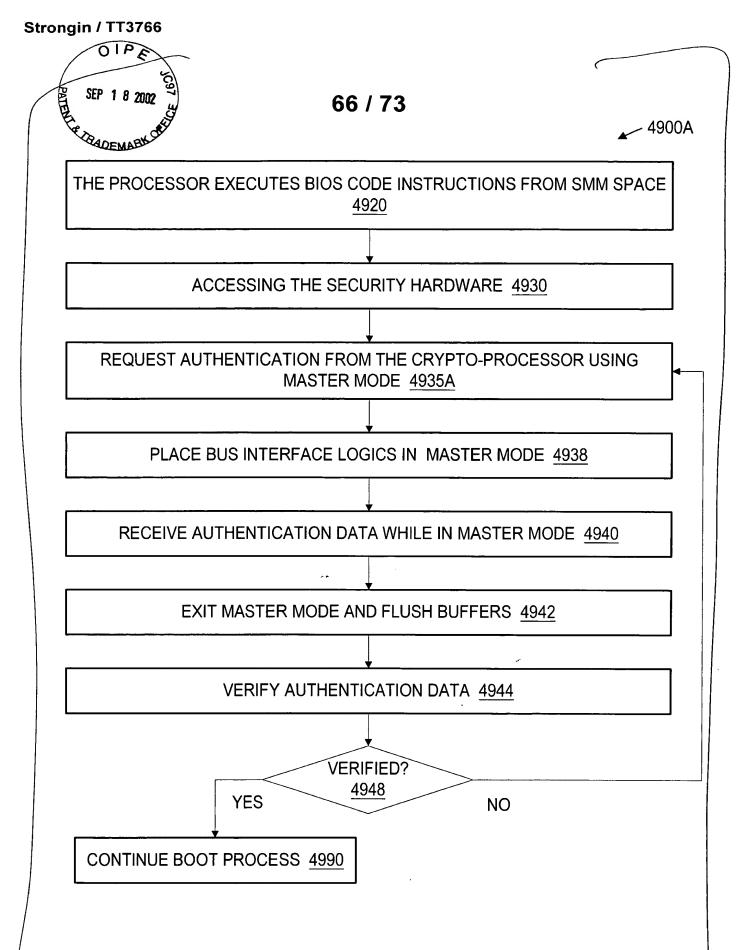


Fig. 38A

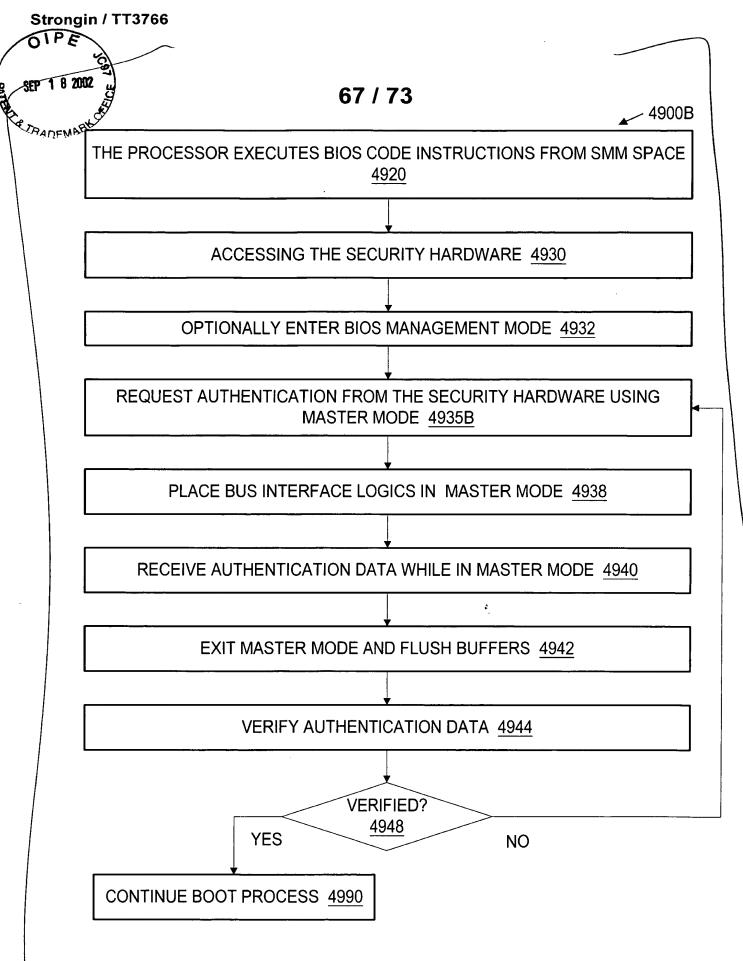
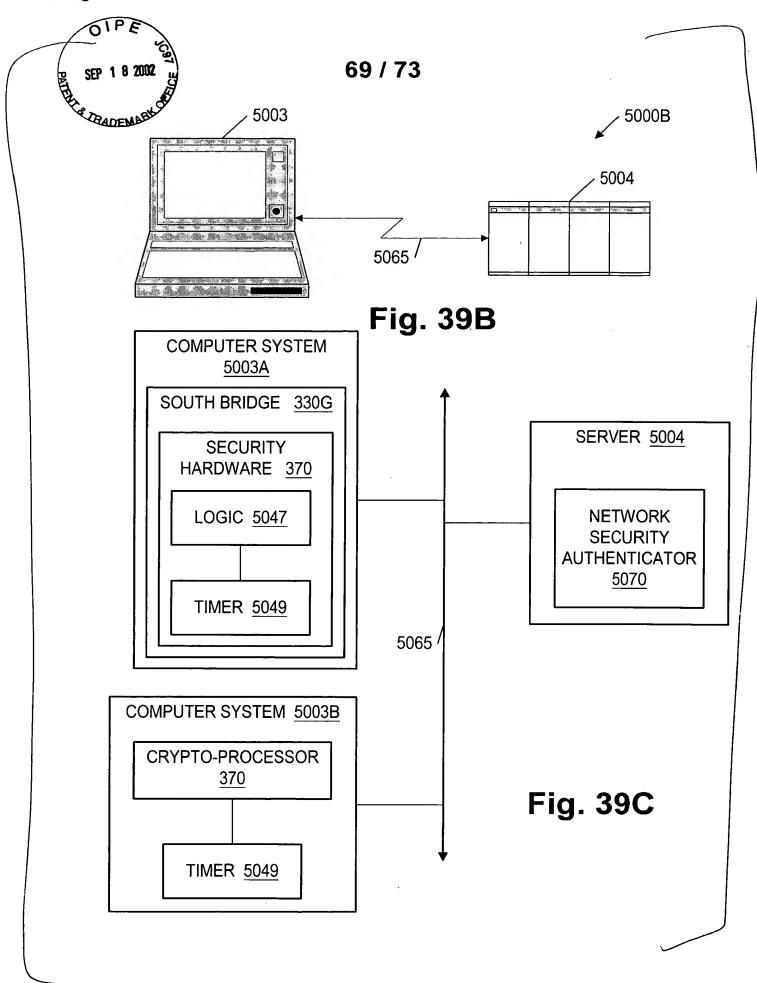
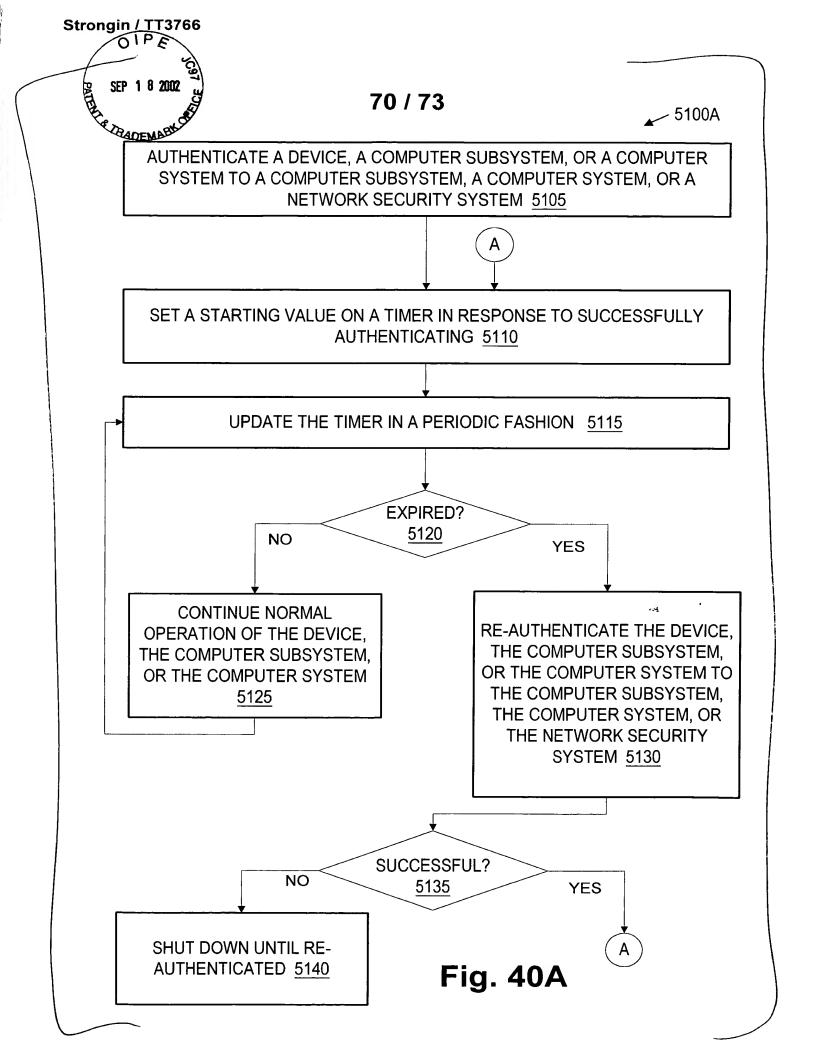
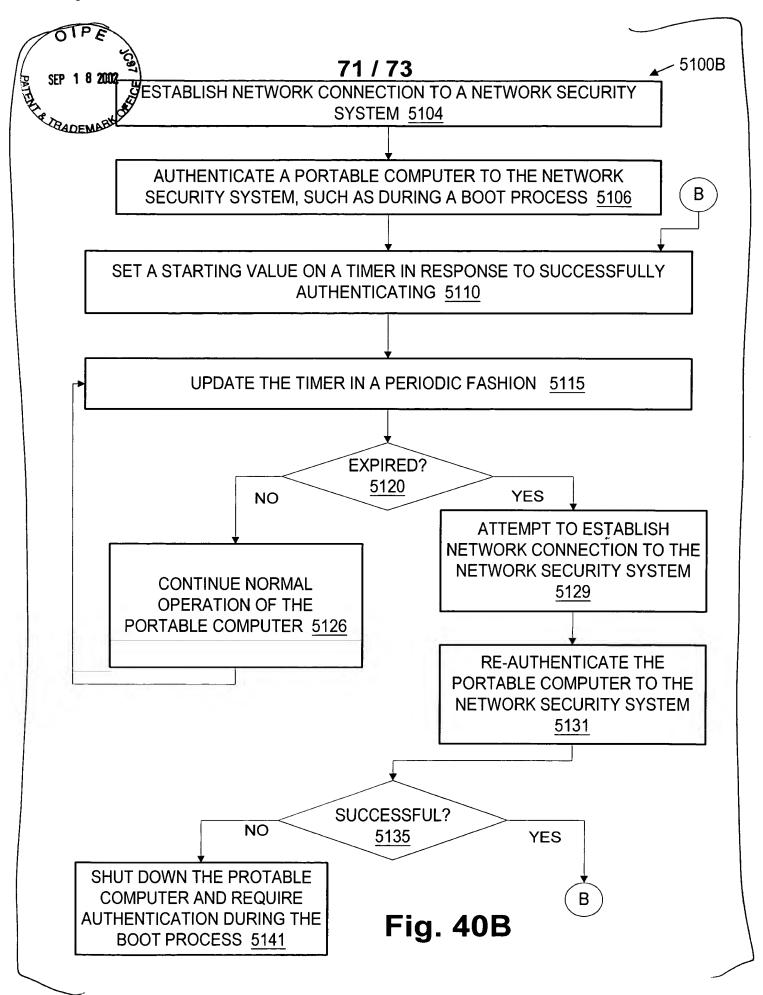
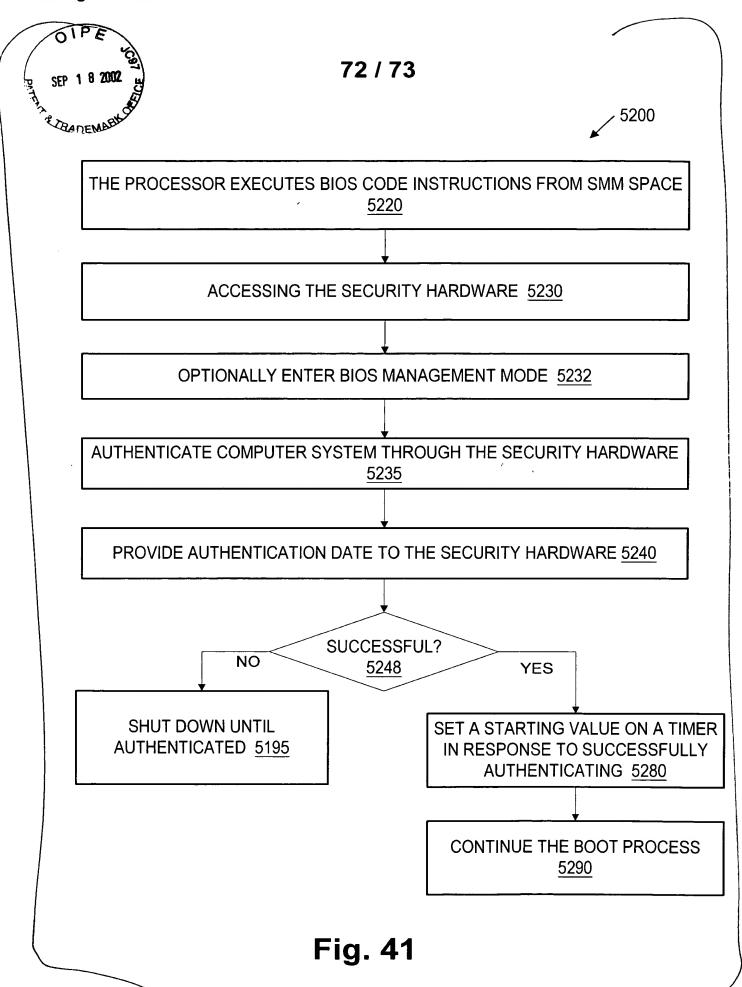


Fig. 38B









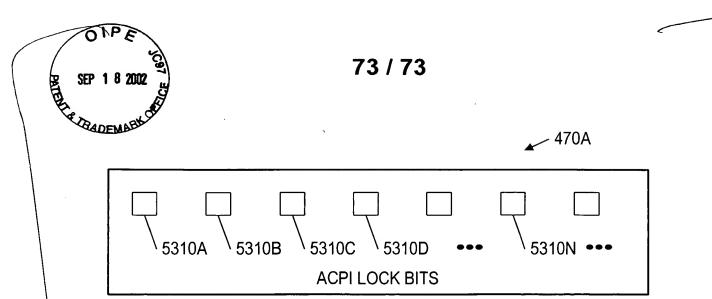


Fig. 42A

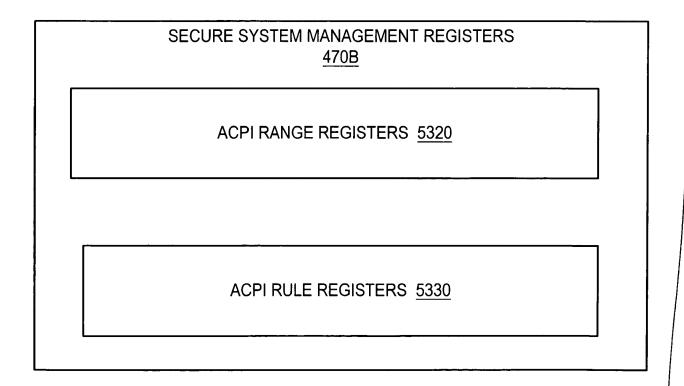


Fig. 42B